Claims

The claims defining the invention are as follows:

1. A method of providing secure transmissions from a biometric smartcard reader, said method comprising the steps of:

encrypting a signal created by a biometric smartcard reader dependent on a smartcard containing biometric data, said smartcard reader able to obtain biometric data directly, said signal comprising access information dependent upon biometric data obtained directly by said biometric smartcard reader from a user and said biometric data contained in said smartcard;

transmitting said encrypted signal to a high security module at a remote location relative to said biometric smartcard reader;

translating by said high security module at said remote location said transmitted signal to another format useable by an access controller; and

controlling an access mechanism using said access controller dependent upon said translated signal.

2. The method according to claim 1, wherein said biometric data comprises fingerprint data.

3. The method according to claim 1 or 2, wherein said biometric data is not transmitted to said high security module at said remote location from said biometric smartcard reader.

4. The method according to claim 1, further comprising the step of providing access using said access mechanism if said translated signal is determined by said access controller to authorise access.

5.. The method according to claim 4, wherein said access mechanism is able to provide access to at least one of a door, portal, computer, network, secure equipment and secure installation.

6. The method according to any one of claims 1-4, wherein said access information comprises at least one of a person's name, a facility code, a company code, an access code, and an issue code.

7. The method according to any one of claims 1-6, wherein said signal is encrypted using triple DES, Skipjack, or AES Rijndael encryption.

8. The method according to claim 1, further comprising the step of encrypting communications between said smartcard and said biometric smartcard reader.

9. The method according to any one of claims 1-8, wherein said high security module translates said encrypted signal to said other format.

10. The method according to any one of claims 1-8, wherein said biometric smartcard reader and said high security module are separated by a distance of up to 1.2 kilometres.

11. The method according to any one of claims 1-8, wherein said smartcard reader and said high security module are separated by a distance of up to 15 metres.

12. The method according to any one of claims 1-11, wherein said translated signal is in a controller-specified format.

13. The method according to claim 12, wherein said controller-specified format is Wiegand format, or clock and data.

14. A system for providing secure transmissions from a biometric smartcard reader, said system comprising:

a biometric smartcard reader for encrypting a signal created by said biometric smartcard reader dependent on said smartcard containing biometric data, said smartcard reader able to obtain biometric data directly, said signal comprising access information dependent upon biometric data obtained directly by said biometric smartcard reader from a user and said biometric data contained in said smartcard, and for transmitting said encrypted signal to a remote location relative to said biometric smartcard reader;

a high security module for receiving said transmitted signal and translating said transmitted signal to another format useable by an access controller; and

an access controller for controlling an access mechanism using said access controller dependent upon said translated signal.

15. The system according to claim 14, wherein said biometric data comprises fingerprint data.

16. The system according to claim 14 or 15, wherein said biometric data is not transmitted to said high security module from said biometric smartcard reader.

17. The system according to claim 14, further comprising an access mechanism providing access if said translated signal is determined by said access controller to authorise access.

18. The system according to claim 17, wherein said access mechanism is able to provide access to at least one of a door, portal, computer, network, secure equipment and secure installation.

19. The system according to any one of claims 16-18, wherein said access information comprises at least one of a person's name, a facility code, a company code, an access code, and an issue code.

20. The system according to any one of claims 16-19, wherein said signal is encrypted using triple DES, Skipjack, or AES Rijndael encryption.

21. The system according to claim 14, wherein communications between said smartcard and said smartcard reader are encrypted.

22. The system according to claim 21, wherein said biometric smartcard reader and said high security module are separated by a distance of up to 1.2 kilometres.

23. The system according to claim 21, wherein said biometric smartcard reader and said high security module are separated by a distance of up to 15 metres.

24. The system according to any one of claims 14-23, wherein said translated signal is in a controller-specified format.

25. The system according to claim 24, wherein said controller-specified format is Wiegand format, or clock and data.

26. An apparatus for providing secure transmissions from a biometric smartcard reader, said apparatus comprising:

a smartcard biometric reader for encrypting a signal created by said biometric smartcard reader dependent on said smartcard containing biometric data, said smartcard reader able to obtain biometric data directly, said signal comprising access information dependent upon biometric data obtained directly by said biometric smartcard reader from a user and said biometric data contained in said smartcard;

means for transmitting using a communications protocol said encrypted signal to a remote location relative to said biometric smartcard reader;

means for decrypting said transmitted signal and translating said decrypted signal at said remote location to another format useable by an access controller, said communications protocol being different to said format useable by an access controller; and

an access controller for controlling an access mechanism dependent upon said translated signal.

27. The apparatus according to claim 26, wherein said biometric data comprises fingerprint data.

28. The apparatus according to any one of claims 26-27, wherein said signal is encrypted using triple DES, Skipjack, or AES Rijndael encryption.

29. The apparatus according to claim 26, wherein said communications protocol is RS232 or RS485.

30. The apparatus according to claim 26, wherein said other format is Wiegand, or clock and data.